

Informe de Gestión de Incidentes Conforme a ISO 27001 – Vulnerabilidad de Inyección SQL

Introducción

Este informe resume la identificación y explotación de una vulnerabilidad de *inyección SQL* en la aplicación Damn Vulnerable Web Application (DVWA).

Descripción del Incidente

Durante la prueba DVWA, se detectó una vulnerabilidad en el módulo "SQL Injection" ID: 1' OR '1'='1 que permite obtener información en el campo de la ID de usuario. Lo que provocó una fuga de datos

Método de Inyección SQL Utilizado

ID: 1' OR '1'='1

introduce una condición que siempre será verdadera lo que devuelve toda la información

Resultado del Ataque

Con la inyección `1' OR '1'='1`, se obtuvo el siguiente resultado:

Nombre: admin, Apellido: admin

Nombre: Gordon, Apellido: Brown

Nombre: Hack, Apellido: Me

Impacto del Incidente

Principalmente se permite

- Que se acceda a la información sin autorización
- Modificación o eliminación de datos críticos.
Esto implica un fuerte riesgo para la confidencialidad, integridad y disponibilidad

Recomendaciones importantes a tener en cuenta la proxima ocasion

1. **Validación de Entradas:** Aplicar validaciones estrictas y usar consultas parametrizadas.
2. **Pruebas de penetración:** para identificar otras fallas
3. **Capacitación:** del personal para que apliquen mejor la seguridad

Conclusión

La detección de esta vulnerabilidad demuestra la necesidad de implementar controles de seguridad robustos y seguir buenas prácticas de ciberseguridad para proteger los activos críticos y garantizar la continuidad del negocio.